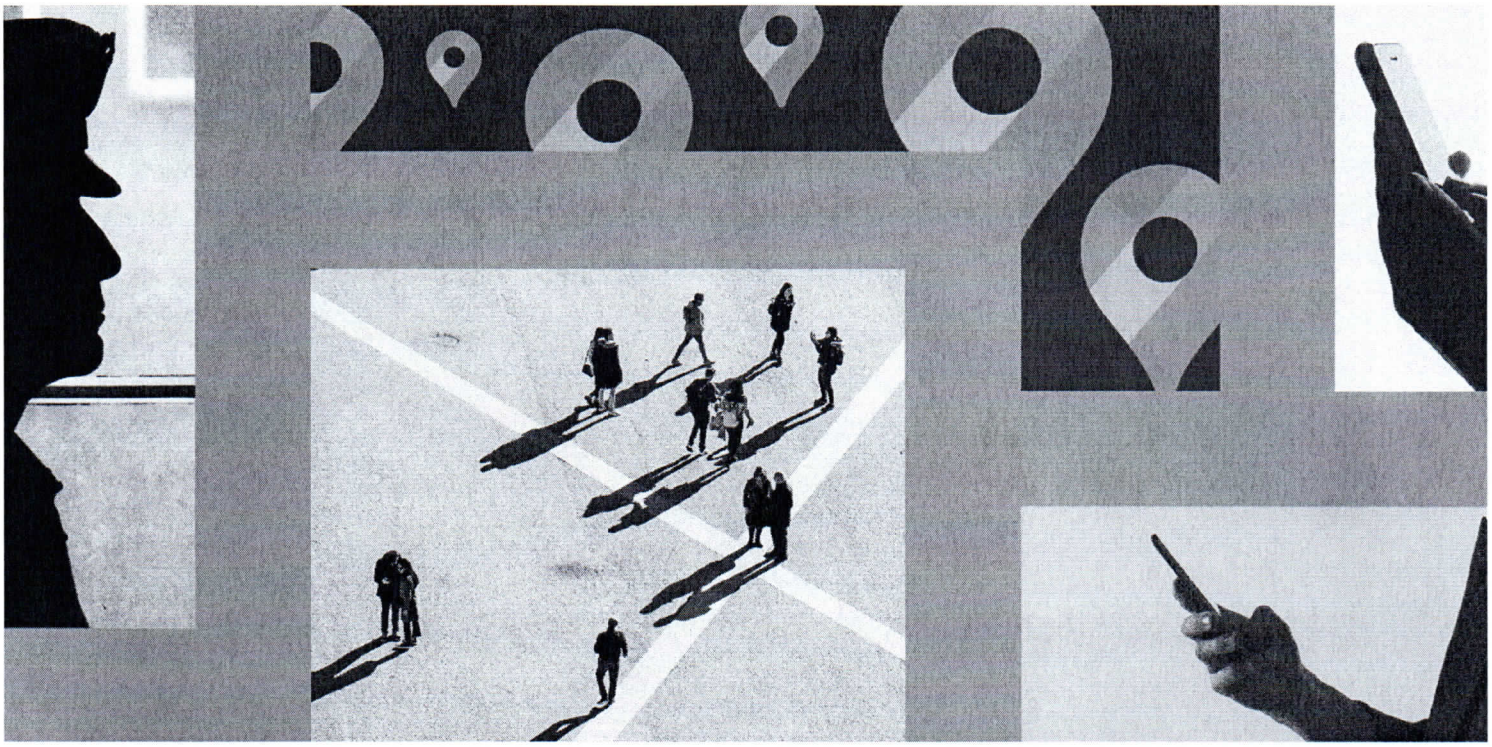
U.S. NEWS

Cellphone dragnet used to find bank robbery suspect was unconstitutional, judge says

A federal judge's ruling that geofence warrants violate the Fourth Amendment could slow the use of surveillance tools based on Google location data.



— Geofence warrants use Google location data to find people who were near a crime scene.

NBC News; Getty Images

March 7, 2022, 4:19 PM CST / Updated March 7, 2022, 7:27 PM CST

By Jon Schuppe

Authorities in Virginia violated the Constitution when they used Google location data to find people who were near the scene of a 2019 bank robbery, a federal judge ruled last week.

The judge found that this policing tactic, which is widely used across the country, breached the Fourth Amendment's protections against unreasonable searches by scooping up information on innocent people without evidence that they might be suspects.

The decision, issued Thursday by Judge M. Hannah Lauck of the U.S. District Court for the Eastern District of Virginia, could make it more difficult for police to use geofence warrants, which draw on tracking data collected by cellphones to find people who were close to a crime scene. The warrants have become popular among law enforcement officers in cases where they have run out of leads using traditional investigatory techniques. The warrants have been used to help solve all sorts of crimes, from burglaries and home invasions to murders and sexual assaults – and to identify people who stormed the U.S. Capitol on Jan. 6, 2021.

But these digital dragnets have raised concerns among defense lawyers and privacy advocates who say the government is secretly collecting data from dozens or more people, most of whom have nothing to do with a crime, in order to find a potential suspect. The critics argue that the warrants put innocent people at risk of wrongful arrest – as happened to a Florida man who was ensnared in a 2019 burglary investigation after riding his bike past the scene.

Albert Fox Cahn, executive director of the Surveillance Technology Oversight Project, a civil rights nonprofit that opposes the use of geofence warrants, said Lauck had issued a "landmark" ruling that could lead to more courts declining law enforcement's requests to use Google location data.

"This is going to be a wake-up call for the judges who have been rubber-stamping these sorts of warrants at the federal and state level," Cahn said.

Law enforcement authorities say geofence warrants are legal because Google users agree to have their location tracked. Police also say they work with Google to receive only anonymized data until they find a device that draws their suspicion. The evidence provided by a geofence warrant alone is not enough to charge someone with a crime, police say.

In the Virginia case, a detective from the Chesterfield County Police Department, assigned to a federal violent crimes task force, sought a geofence warrant after three weeks of trying to identify a gunman who walked to a bank in Midlothian, forced a worker to open a safe and walked out with $195,000. Security footage showed that when the suspect arrived at the bank, he was holding a cellphone to his ear. The detective requested a warrant for Google's location data from all the cellphones that had been in a 150-meter radius (about 164 yards) of the bank during the heist. A local magistrate approved the warrant.

Google provided location data, but not identifying information, for 19 devices in the area. The detective gradually narrowed the list to three devices, and Google provided information about the people whose names were associated with them. That led investigators to Okello Chatrie, 27, who was charged with armed robbery in September 2019. Chatrie has remained in jail since then and has pleaded not guilty.

His lawyers, including Michael Price, the lead litigator of the National Association of Criminal Defense Lawyers' Fourth Amendment Center, argued that the geofence warrant violated the Constitution and that the information police got from it should be thrown out.

Price and Chatrie's public defender, Laura Koenig, declined to comment on Lauck's ruling. So did the U.S. Attorney's Office in the Eastern District of Virginia and the Chesterfield County Commonwealth's Attorney's Office. The detective who sought the warrant and the magistrate who approved it could not immediately be reached for comment.

Google released a statement saying the company was reviewing the court's decision. "We vigorously protect the privacy of our users," a spokesperson said, "including by pushing back on overly broad requests, while supporting the important work of law enforcement.

Chatrie's challenge prompted the deepest courtroom examination of geofence warrants to date, including hearings that explored the details of Google location data, how law enforcement negotiates with Google for that information and what investigators do with it.

The number of geofence warrants police submitted to Google has risen dramatically. In 2018, Google received 982 geofence warrants from law enforcement; in 2020 that number surged to 11,554, according to the most recent data provided by the company. Google now gets geofence warrants from agencies in all 50 states, Washington, D.C., and the federal government.

Until now, geofence warrants have largely gone uncontested by U.S. judges, with rare exceptions. They include two federal magistrates in Illinois who refused requests for geofence warrants in 2020, a federal magistrate in Kansas who turned down a request last year and a judge in Fairfax, Virginia, who declined a warrant request last month.

The Chatrie case was the first to comprehensively examine the pros and cons of geofence warrants; it included arguments and experts representing the government and Chatrie, as well as testimony from Google executives. The process lasted more than two years.

In the end, Lauck sided with Chatrie – but with a catch.

Lauck wrote in her March 3 decision that the way authorities used the geofence warrant – capturing data on a large number of people within an area that included a church, a restaurant, a hotel and an apartment complex, with little judicial oversight – "plainly violates the rights enshrined in" the Fourth Amendment. Lauck noted that the warrant "swept in unrestricted location data for private citizens who had no reason to incur Government scrutiny." That included one person who didn't appear to actually be in the 150-meter radius.

The judge also seemed troubled by the testimony of an expert, working for Chatrie, who was able to find the likely identities of three people whose location data was provided in response to the warrant by identifying their likely homes, tax records and social media accounts.

But Lauck stopped short of invalidating the evidence produced by the warrant, which could have made it difficult to prosecute Chatrie. Instead, Lauck ruled that the evidence could stand in this case, saying the detective who sought the warrant was not at fault because he had no one telling him it was unconstitutional; he had successfully sought geofence warrants in past cases and had consulted with prosecutors. Chatrie, therefore, won't benefit from Lauck's ruling. He is awaiting trial.

Although Chatrie can still be prosecuted using evidence obtained from the geofence warrant, Lauck's ruling could make it more difficult for police to obtain the warrants in the future – and

more likely that judges will suppress evidence obtained from them, experts said.

Jennifer Lynch, surveillance ligation director at the Electronic Frontier Foundation, a nonprofit digital rights group, said she believed other courts will consider Lauck's opinion in deciding whether to approve the geofence warrants.

"There are more and more of these warrant requests going around, and judges are starting to look more closely at them, and they are becoming aware of the problem with them," Lynch said.

Jake Laperruque, senior policy counsel at The Constitution Project at the Project on Government Oversight, said Lauck's ruling could make it easier for defendants to challenge not only geofence warrants but other kinds of mass surveillance tools.

Lauck "made it pretty clear that this type of dragnet measure on its face without proactive efforts to limit it is unacceptable," Laperruque said.

Lauck wrote that her decision was part of the judiciary's "ongoing efforts to apply the tenets underlying the Fourth Amendment to previously unimaginable investigatory methods" powered by the massive amount of location data collected by Google and other technology giants.

The judge stressed that her ruling was not meant to say whether geofence warrants should ever be used. She suggested that there might be a way to use them without violating the Fourth Amendment, perhaps by limiting their scope and by seeking more court input during the process. She cited a Washington, D.C., case in which a federal court in December required law enforcement to request additional court approval before seeking personal information linked to devices that belonged to likely suspects.

In the end, the judge wrote, the future of geofence warrants should be taken up by lawmakers. She noted that there is no law that prevents tech companies from collecting and using vast amounts of data from customers. She cited a bill in New York that seeks to ban the use of geofence warrants.

"Thoughtful legislation could not only protect the privacy of citizens, but also could relieve companies of the burden to police law enforcement requests for the data they lawfully have," Lauck wrote.

Jon Schuppe